

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. Please amend claims 1-7, 9, 11, 14, 17, 20, 22 as follows.

Listing of Claims

1. (Currently Amended) A digital private key protection device, comprising
a digital private key storage means containing a user's digital private key;
a cryptographic engine;
a communications port for receiving digital data from an external device, and for transmitting data to said external device;
a trusted display means for displaying said received digital data;
a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data; wherein said cryptographic engine is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device.

2. (Currently Amended) A digital private key protection device according to claim 1, wherein said digital private key storage means contains a trusted public key and a plurality of user's public keys signed by said ~~trusted-digital~~ private key; and said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of said user's public key and then decrypts said received data using said verified predetermined user's public key and causes said trusted display to indicate whether said user's private key was used to sign said received digital data.

3. (Currently Amended) A digital private key protection ~~system-device~~ according to claim 1, wherein said ~~signed-received~~ digital data ~~is~~ includes a digital certificate for said digital data created using a user's private key or a digital private key or a secret key of a digital private key protection device.

4. (Currently Amended) A digital private key protection system-device according to claim 1 further comprising an audit means wherein signed data is not transmitted external of said digital private key protection device until a said ~~encryption~~ cryptographic engine process is audited by said audit means.

5. (Currently Amended) A digital private key protection system-device according to claim 2 further comprising an audit means wherein signed data is not displayed until a said cryptographic engine ~~encryption~~ process is audited by said audit means.

6. (Currently Amended) A digital private key protection system-device according to claim 1 wherein said digital private key protection device further comprises a private key protection device private key storage means wherein digital data signed by said private key protection device after operation of said user operable input means is further signed by said private key of said private key protection device.

7. (Currently Amended) A digital private key protection device according to claim 1 wherein said digital private key storage means contains a predetermined digital private key protection device's public key; such that when said communications port receives signed digital data from an external device which may or may not have been signed by a said predetermined digital private key protection device;

said cryptographic engine decrypts said received data using said predetermined digital private key protection device's public key to verify whether said digital private key protection device's predetermined digital private key was used to ~~sign~~ encrypt said received digital data.

8. (Original) A digital private key protection device according to claim 7 wherein said display means indicates whether said digital private key protection device's private key was used to encrypt said received data.

9. (Currently Amended) A digital private key protection device according to claim 1 further comprising a public key storage means containing a plurality of user's public keys; and

said received digital data contains information that predetermines which user's public key is used to sign said received data that is transmitted external of said digital private key protection device to ~~said~~ a predetermined user.

10. (Original) A digital private key protection device according to claim 1 wherein said cryptographic engine is trusted to decrypt digital data using said user's digital private key and passing decrypted digital data to said display means for display of said received digital data.

11. (Currently Amended) A digital private key protection device according to claim 10 wherein ~~said cryptographic engine does not decrypt signed digital data~~ decrypted information is not released external to said device unless said user operable input means is operated.

12. (Original) A digital private key protection device according to claim 10 wherein said communications port can not transmit said decrypted digital data.

13. (Original) A digital private key protection device according to claim 12 wherein said communications port can not transmit said decrypted digital data unless said user operable input means is operated.

14. (Currently Amended) A digital private key protection device according to claim 1 wherein said digital private key storage means also contains a digital shared secret symmetric key wherein said cryptographic engine is trusted to only apply said digital shared secret symmetric key to encrypt data only if said user operable input means is operated and also trusted to communicate said ~~signed~~ encrypted data external of said digital private key protection device.

15. (Previously Presented) A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines how said encryption engine should encrypt or decrypt respectively.

16. (Previously Presented) A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines which protocol is used by said device to communicate encrypted or signed data external of said device.

17. (Currently Amended) A digital private key protection device according to claim 1, wherein said trusted display means is external to said device and controlled by said device for displaying data transmitted from said communications port in a trusted manner.

18. (Previously Presented) A digital private key protection device according to claim 1, wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner.

19. (Previously Presented) A digital private key protection device according to claim 1, further comprising identification and authentication means actuated by said user in a predetermined manner.

20. (Currently Amended) A digital private key protection device according to claim 18 further comprising an audit means which audits said actuation of said user ~~identification~~ operable input means.

21. (Previously Presented) A digital private key protection device according to claim 1, wherein said digital private key storage means is removable from said device.

22. (Currently Amended) A digital private key protection device according to claim 1, wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said PKPD-digital private key protection device using the user's private or other keys as identified by the request, but excluding the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.

Application No. 09/856,813
Paper Dated March 7, 2005
In Reply to USPTO Correspondence of November 5, 2004
Attorney Docket No. 1376-010862

23. (Original) A digital private key protection device according to claim 22 wherein said device displays a description of said request to the user and, only if the user operates said user operable input means, does said device carry out said request.